Security and Privacy End of Chapter Exercises

**7.1. Briefly describe the three main types of threat that have to be considered when planning how to secure a software product against cyberattacks.**

The three main types of threat include availability threats, integrity threats and confidentiality threats. Availability threat is when an attacker attempts to deny access to the system for legitimate users. Integrity threat is when an attacker attempts to damage the system or its data. Confidentiality threats is when an attacker tries to gain access to private information held by the system.

**7.2. Explain in your own words what you understand by an SQL injection attack. Explain how you can use data validation to avoid such attacks.**

SQL injection attack is a web security vulnerability that allows an attacker to interfere with queries of an application in its database. Malicious SQL statements are inserted into an entry field for execution. With the help of this attack, attackers can retrieve hidden data.

The validation process helps verify whether or not the type of input submitted by a user is allowed. Input validation makes sure it is the accepted type, length, format, and so on. Only the value which passes the validation can be processed. It helps counteract any commands inserted in the input string.

**7.3. What do you think are the advantages and disadvantages of using a special-purpose device rather than a mobile phone in two-factor authentication? (Hint: Think about the problems of using a mobile phone as an authentication device.)**

The advantage of using a special purpose device that calculates a code is that this method can be used in the absence of a cellular coverage or internet access. Mobile phones can not be used in two-factor authentication if there is no cellular coverage. Moreover, mobile phones can be easily stolen, lost or the battery can discharge in which case the code cannot be accessed. Attackers can also easily intercept sms messages and can also steal phone numbers. However, the advantages of a mobile phone compared to the special purpose device is that mobile phone two-factor authentication is easier to use as the user just has to input code from SMS.

**7.4. Suggest, giving reasons, appropriate forms of authentication for the following products:**

**a. An e-learning product for teachers and students, funded by advertising, that allows users to recommend videos and other learning material on a range of topics.**

A knowledge-based authentication based on a password would be most suited for the e-learning product since the e-learning product does not contain sensitive user information. It has learning material and a password for authentication is enough.

**b. A personal finance app for mobile devices that can automatically transfer funds between different accounts based on rules set up by the user.**

Two-stage authentication/mutlifactor would be best for a personal finance app that uses phone-based authentication as well as passwords and possibly personal questions. This makes it harder for attackers to break into the system.

**c. A human resources product for businesses that helps manage the process of recruiting new staff.**

**7.5. What is the difference between symmetric and asymmetric encryption? Why do we need both encryption methods?**

In symmetric encryption, the same encryption key is used to encode and decode sensitive information so the key has to be shared between the two users. On the other hand, asymmetric encryption doesn’t require keys to be shared because it uses different keys for encrypting and decrypting messages. Both encryption methods are needed because asymmetric encryption takes about 1000 times longer than symmetric encryption for the same level of security. Therefore, asymmetric encryption is only used for encoding relatively short messages. Therefore, we need both forms of encryption.

**7.6. Explain why it is normally preferable to use a database's built-in encryption support rather than implement your own application-level encryption.**

It is preferable to use a database’s built-in encryption because we do not need to write any encryption/decryption code when using the database encryption. It is also easier to use the built in encryption in the database. On the other hand, implementing a good trustworthy encryption on the client side (application-level) is complex and expensive with the possibilities of making mistakes. This could lead to a less secure system. Moreover, application-level encryption can slow down the performance of the system. This could lead to users not using the software in itself. Finally, implementing client side encryption means, the developer has to provide key management functionality which involves writing extra code to integrate the application with a key management system.

**7.7. Explain how encryption keys are securely exchanged in the TLS protocol.**

In TLS protocol, the TLS encryption depends on a digital certificate (issued by the CA) that is sent from the web server to the client. The identity of the organization is encoded in the digital certificate. In order to exchange encrypted information, an encryption key is established that both the client and server use. The server sends the client a digital certificate that includes the server’s public key. The server also encrypts a long random generated number using its private key which it then sends to the client. The client decrypts this using the server’s public key and also generates a long number which it encrypts using server’s public key and sends it to the server. The server decrypts it using its private key. This way both the client and server have two long randomly generated number. The client and server independently compute the key that will be used to encrypt messages using a symmetric approach. All client—server traffic is then encrypted and decrypted using that computed key without having to exchange the key itself.

**7.8. What are the problems in maintaining confidential information that, by law, has to be kept for a number of years? How can a key management system help with these problems?**

The problem in maintaining confidential information is that businesses have to manage thousands of encryption keys that are used to encrypt confidential data. To maintain confidential data, businesses have to make sure that the encryption keys are securely generated, stored and accessed by authorized users. If businesses get something wrong in the key management system then unauthorized users may be able to access the keys and get access to confidential data. Moreover, if an encryption key is lost, then the encrypted data may be permanently inaccessible.

A key management system helps with these problems as it uses a specialized database to securely store and manage encryption key, digital certificates, and other confidential data.

**7.9. Why is it difficult to establish a set of privacy standards that can be applied internationally in software products?**

Since people have differing views and opinions on privacy, it is impossible to establish privacy standards that can be applied internationally. Different countries and cultures have different ideas what about what information should and should not be private. Therefore, setting a set of privacy standards for everyone to follow is hard.

**7.10. A Chinese e-commerce company decides to expand its, business into the European Union. It proposes to use a local cloud vendor for application server provision but to transfer user information to servers in China for analysis. Explain why this information transfer might be illegal, according to data protection legislation. (Hint: Look at the issues related to keeping data anonymous.)**